UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case Number 09-20023-BC
Honorable Thomas L. Ludington

D-10 JOANNE TRAGAS,

Defendant.
_____/

ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS, DENYING DEFENDANT'S MOTION TO PERMIT DEFENDANT TO ACCESS LAPTOP COMPUTER TO REVIEW DISCOVERY, STRIKING THE GOVERNMENT'S SUPPLEMENTAL BRIEF AND DIRECTING THE CLERK TO REMOVE THE IMAGES FROM THE DOCKET, DETERMINING EXCLUDABLE DELAY, AND SCHEDULING FINAL PRETRIAL CONFERENCE AND TRIAL DATES

Now before the Court is Defendant Joanne Tragas' motion to suppress [Dkt. # 142] filed on January 11, 2010. Defendant Tragas seeks suppression of all communications seized from a specified laptop computer.[1] On February 1, 2010, the government filed a response [Dkt. # 152]; and on February 23, 2010, Defendant filed a reply [Dkt. # 163]. The government filed a sur-reply brief [Dkt. # 165] on February 26, 2010. The Court held a hearing on the motion on March 8, 2010. Subsequent to the hearing, the government filed a supplemental brief [Dkt. # 173]. The supplemental brief, however, will be stricken because the government did not seek leave to file the brief nor provide any justification for the belated filing. Perhaps most importantly, Defendant has

[1] While Defendant Tragas' reply brief also refers to a seizure of "Mr. Hunter's cellular phone," any issues regarding the phone are not raised in Defendant's motion, elaborated upon in the reply brief, and were not pursued at the hearing. Thus, any issues regarding the seizure of "Mr. Hunter's cellular phone" are not properly before the Court.

not had an opportunity to respond to the supplemental brief. Nonetheless, as further explained below, Defendant's motion will be denied for lack of standing under the Fourth Amendment.

I

On July 20, 2009, a criminal complaint was sworn by a federal agent before Magistrate Judge Charles E. Binder as to Defendant Joanne Tragas. The agent stated, in part, the following:

> . . .
>
> 2. On December 11, 2008, as a result of an on-going local investigation, Eugene Watkins, Derrick James Moore, and Ashley Rebecca Allen were arrested for felony larceny by the Saginaw County Sheriff's Department in the parking lot at the Meijer store on Tittabawassee Road in Saginaw, Michigan. They had fourteen counterfeit Visa gift cards in their possession, some of which they had just used to purchase various items from that Meijer store.
>
> . . .
>
> 7. [In a later interview] . . . Allen stated . . . that she used Visa gift cards given to her by Watkins to purchase [various items from various stores in Saginaw, Flint, and Ypsilanti, Michigan.] Allen . . . had a truck [used for driving Moore and Watkins to various stores and for transporting large items.]
>
> 8. Allen explained that Moore and Watkins obtain the counterfeit Visa gift cards from a person in Detroit. . . . Though she did not know the name of the person who supplies the cards to Watkins, she was able to identify the person [as Brian Denard Coleman] from a group of driver's license photographs. . . .
>
> . . .
>
> 11. [After a search of his residence in December 2008,] Coleman . . . offered to cooperate with the continuing investigation. . . . Coleman . . . admitted that . . . he had been purchasing counterfeit cards from . . . twin brothers, Dion and Dionte Hunter . . . [who] generally drive a white BMW or a white Range Rover. . . .
>
> . . .
>
> 13. Coleman explained that he was instructed by the Hunters to return the fraudulent Visa gift cards to them when the cards no longer worked so the Hunters could reencode them with a new account number and sell them again. . . .
>
> . . .
>
> 16. I ran Dion Richard Hunter's criminal history through NCIC and learned that Dion was arrested in June of 2008 by the Southfield, Michigan Police Department . . . [while] driving a 2007 white 750LI BMW registered to Stacy Pugh of Detroit, Michigan.

. . .

18. On March 12, 2009, I spoke to the service manager for the BMW dealership in Farmington Hills, Michigan. The service manager told me that the dealership had serviced the white BMW registered to Pugh on March 10, 2009. He said that Dion Hunter had brought the vehicle in for maintenance.

19. On March 13, 2009, Pugh told me that she had leased the BMW through a broker to a person known to her only as "Twin." The last lease payment Pugh received for the vehicle was in January of 2009 . . . . Pugh thereafter contacted BMW and reported the vehicle missing. Pugh gave me consent to search the vehicle, which had already been recovered from the parking lot at Dion Hunter's apartment complex by a repossession company. The "repo" company also gave consent to search the BMW. Five Visa gift cards, a laptop computer, a credit card encoder, credit card receipts, two photographs of Dion and Dionte Hunter with other individuals, and mail . . . addressed to Dion . . . and . . . Dionte Hunter were found during the search of the BMW.

. . .

22. On March 20, 2009, the apartment rented by Dion Hunter was searched pursuant to a federal search warrant. . . . [A] Wal-Mart gift card was found . . . , [which had been] purchased fraudulently on February 20, 2009 at a Wal-Mart in Columbus, Ohio[, according to Wal-Mart's asset protection unit. The Wal-Mart card, along with one other Wal-Mart card,] were used to buy a total of eighteen $100 American Express gift cards from Wal-Mart's internet site, all of which were mailed to Joanne Kolomvakou at 1918 Cape Coral Parkway in Cape Coral, Florida. The email account used to order the gift cards is registered to jtragas@yahoo.com.

23. On or about February 2, 2009, the sale of a residence at 1918 Cape Coral Parkway in Cape Coral, Florida was closed. The title is in the name of Giannoula Kolomvakou of Sparta, Greece. . . . In the course of preparing the paperwork for the transaction, the title company was told that Joanne Tragas is the "English" version of the name Giannoula Kolomvakou.

24. Based on the information I have acquired during this investigation, I have reason to believe that one person is using the name Joanne Tragas, Joanne Kolomvakou and Giannoula Kolomvakou. In fact, on or about July 7, 2009, a Secret Service agent observed packages addressed to Joanne Tragas and Joanne Kolomvakou on the porch of the residence at 1918 Cape Coral Parkway, Cape Coral, Florida.

25. The laptop computer seized from the BMW has been examined pursuant to a federal search warrant by an agent trained in computer forensics. That examination has revealed a series of communications between that computer and a computer used by Joanne Tragas. One of the significant communications occurred on or about January 21, 2009, when a message received by the Hunter computer from the Tragas computer stated that the sender of the message was flying to the United States in nine days to close on a house in Florida. Another of the more significant communications occurred on February 20, 2009, when the computer seized from the BMW was used to send the sixteen digit card numbers and pin

numbers for two $1,000 Wal-Mart gift cards to Tragas's computer.

> 26. Based on the above, it appears that the means to use the two $1,000 gift cards purchased by the Hunter twins in Columbus, Ohio was transferred to Tragas and that Tragas used those cards to buy American Express gift cards. Moreover, it appears from other communications found on the computer seized from the BMW that the information needed to enable Tragas to access the $2,000 on those gift cards was sent to her computer because she had sent information needed to encode gift cards with stolen credit card numbers to email accounts associated with the computer seized from the BMW. The information sent from the Tragas computer to the Hunter computer included BINs and "dumps." A BIN is a bank identification number, consisting of the first six numbers of a sixteen digit credit or debit card number. Each BIN is unique to the card-issuing financial institution. "Dumps" is the term applied to the data encoded in the magnetic strip on the back of a credit and debit cards. The information sent from the Tragas computer to the Hunter computer could be used by the recipient to manufacture the type of counterfeit access devices sold by the Hunters to others and described above.
>
> 27. The communications recovered from the laptop seized from the BMW include discussions between that computer and Tragas's computer regarding the means of paying for the BIN and dump information. Messages sent from the Tragas computer to the Hunter computer directed that payment be sent in the form of gift cards, by wire transfer, and by deposits into a Bank of America account [in the name of Joanne Tragas]. . . .
>
> . . .
>
> 29. The communications recovered from the computer seized from the BMW suggest that Tragas has been sent substantial amounts of money by various means for the BIN and "dumps" information transferred from the Tragas computer to the Hunter computer. Based on my analysis of the communications to date, it appears that wire transfers, gift card information, and deposits into her Bank of America account totaling over $100,000 have been received by Tragas from the Hunters, and people acting at their direction, for the information she has provided to promote the access device fraud scheme.
>
> . . .

Crim. Compl., July 20, 2009.

In count one of the fourth superseding indictment [Dkt. # 125], the government charges Defendant Tragas and her nine co-defendants with a conspiracy under 18 U.S.C. § 1029(b)(2), to commit violations of 18 U.S.C. §§ 1029(a)(1)–(5). Each of those statutory provisions, respectively, applies to an individual who "knowingly and with intent to defraud," engages in the following acts: (1) "produces, uses, or traffics in one or more counterfeit access devices"; (2) "traffics in or uses one

or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period"; (3) "possesses fifteen or more devices which are counterfeit or unauthorized access devices"; (4) "produces, traffics in, has control or custody of, or possesses device-making equipment"; and (5) "effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000." 18 U.S.C. §§ 1029(a)(1)–(5).

In particular, count one the indictment alleges that Defendant Tragas obtained stolen credit and debit card account information from others, which she repeatedly sold to, inter alia, co-Defendants Dion and Dionte Hunter. Count one alleges that on December 29, 2005, Defendant Tragas used a computer to obtain registration information for a forum which operated a website used to traffic in stolen credit and debit card information called "scandinaviancarding.com." In turn, co-Defendants Dion and Dionte Hunter paid Defendant Tragas for the information with fraudulently-obtained, but genuine, gift cards.

In counts two, four, five, six, and seven of the indictment, the government charges Defendant Tragas and co-Defendant Dionte Hunter with violations of 18 U.S.C. §§ 1952(a)(1) and (3) on or about April 22, 2008, on or about May 31 to June 2, 2008, on or about June 6 to 14, 2008, on or about June 29 to July 1, 2008, and on or about August 20, 2008, respectively. The statutory provisions provide:

> (a) Whoever travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce, with intent to--
>
> (1) distribute the proceeds of any unlawful activity; or
>
> . . .
>
> (3) otherwise promote, manage, establish, carry on, or facilitate the promotion, management,

establishment, or carrying on, of any unlawful activity. . . .

18 U.S.C. §§ 1952(a). Similarly, counts three and eight of the indictment charge Defendant Tragas and co-Defendants Dion and Dionte Hunter with violations of 18 U.S.C. §§ 1952(a)(1) and (3) on or about May 16, 2008, and on or about February 20, 2009, respectively.

Count nine charges Defendant Tragas and co-Defendants Dion and Dionte Hunter with violations of 18 U.S.C. § 1344 from December 2006 to on or about July 20, 2009, that is, Defendants "aided and abetted by each other and by others . . . did knowingly execute and attempt to execute a scheme or artifice to defraud a financial institution, that is Chase Bank, and to obtain some of the moneys, funds, credits and assets owned by and under the control of Chase Bank, by means of false and fraudulent pretenses and representations, in that [Defendants] used, attempted to use, and caused the use of unauthorized, counterfeit access devices to obtain access to the lines of credit associated with genuine credit card accounts issued by Chase Bank. . ."

Similarly, count eleven charges Defendant Tragas and co-Defendants Dion and Dionte Hunter, Tristan Harrison, and Demario Wilson with violations of 18 U.S.C. § 1343 from April 8, 2006 to on or about July 16, 2009, that is, Defendants "aided and abetted by each other and by others . . . , having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, did knowingly transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, various writings, signs and signals in the form of wire transfers of funds and Internet communications, for the purposes of executing such scheme and artifice, and thereby affected a financial institution . . . ."

Finally, counts ten and twelve only charge violations of the law against co-Defendants of

Defendant Tragas.

II

Defendant Tragas raises three primary arguments in her motion to suppress. The first two arguments will be addressed in tandem, followed by the third. First, Defendant Tragas contends that all of the communications stored on the laptop computer seized from the BMW informally leased to co-Defendants Dion and Dionte Hunter by Stacy Pugh should be suppressed because the search of the vehicle was not conducted pursuant to a warrant, Pugh did not have the authority to consent to a search of the vehicle leased to the Hunters, and the search of the vehicle exceeded the scope of the consent given. Defendant Tragas asserts that a consent form signed by Pugh only gave consent to search the vehicle and to seize evidence consisting of a "counterfeit access device."

Second, Defendant Tragas contends that the communications should be suppressed because the laptop computer was initially searched without a warrant. She asserts that she was "unknown" to law enforcement prior to the search and seizure of the laptop computer. She further asserts that the affidavit in support of the search warrant for the laptop computer contained information that could only have been obtained through a prior, warrantless search of the laptop computer. Notably, this is inconsistent with the criminal complaint sworn by the federal agent, which suggests that the agent learned of the email address jtragas@yahoo.com on or about March 20, 2009, subsequent to the search of co-Defendant Dion Hunter's apartment. *See* Crim. Compl. ¶¶ 22-23.

In response, the government contends that Defendant Tragas lacks the legitimate expectation of privacy required to give her standing under the Fourth Amendment to challenge the search of the laptop computer. The government emphasizes that Defendant Tragas does not allege that she was the person who used the seized laptop computer and had the ability to exclude others from access.

The government reserves the right to address the legality of the search if Defendant Tragas can establish standing.

"Because Fourth Amendment rights are "personal," the central inquiry in any suppression hearing is whether the defendant challenging the admission of evidence has shown a legitimate expectation of privacy in the place searched or the thing seized." *United States v. King*, 227 F.3d 732, 743-44 (6th Cir. 2000) (citing *Rakas v. Illinois*, 439 U.S. 128, 140 (1978), *Katz v. United States*, 389 U.S. 347, 353 (1967), *Minnesota v. Olson*, 495 U.S. 91, 96-97 (1990), and *United States v. Kincaide*, 145 F.3d 771, 779 (6th Cir. 1998)). In *King*, the Sixth Circuit Court of Appeals explained that "[a] determination of whether a legitimate expectation of privacy exists involves a two-part inquiry":

> First, we ask whether the individual, by conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private. . . . Second, we inquire whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable.

Id. (internal citations and quotations omitted). "Whether a legitimate expectation of privacy exists in a particular place or item is a determination to be made on a case-by-case basis." *Id.* (internal citations and quotations omitted). Additionally, "suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence." *Alderman v. United States*, 394 U.S. 165, 171-72 (1969); *see also United States v. Salvucci*, 448 U.S. 83, 85 (1980) (overruling the "automatic standing" rule).

Defendant Tragas contends that *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), vacated en banc on ripeness grounds, 532 F.3d 521 (6th Cir. 2008), stands for the proposition that "e-mails held by an ISP" are similar to sealed letters, in which the sender maintains an expectation

of privacy, requiring that law enforcement obtain a warrant based on probable cause to search the emails. Defendant Tragas further asserts that there can be no dispute that she and the Hunter co-Defendants expected that their emails would be kept private. Significantly, as the government notes, an individual "would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter." *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (quoting *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995)).

Defendant Tragas also argues that she has "standing" based on the traditional formulation of that concept. *See Warshak*, 490 F.3d at 465 ("To establish standing, a plaintiff must allege (1) an injury that is (2) fairly traceable to the defendant's allegedly unlawful conduct and that is (3) likely to be redressed by the requested relief.") (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). However, as the government emphasizes, the "standing" requirements highlighted in *Warshak* are not specific to the Fourth Amendment "standing" required to seek the suppression of evidence in a criminal case. Thus, *Warshak* does not inform the analysis as to standing under the Fourth Amendment.

Finally, Defendant Tragas' third argument is that she has a property interest and an expectation of privacy in all communications stored on the laptop computer pursuant to the Stored Communications Act, 18 U.S.C. § 2703(a)–(b).[2] Specifically in response to this argument, the

[2] Subsections (a) and (b) of 18 U.S.C. § 2703 provide in full:

> (a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure

government contends that the provisions of the statute relied upon by Defendant Tragas apply to "providers of electronic communications services." The government emphasizes that the seized laptop computer was examined by an agent trained to conduct forensic computer searches and that the communications service provider did not participate in the search, making § 2703(a) and (b) irrelevant.

Defendant Tragas also makes a reference to the Federal Wiretap Statute, 18 U.S.C. § 2510 in her motion to suppress. In response, the government asserts that Defendant Tragas cannot establish that she is an "aggrieved person" within the meaning of the statute. *See* 18 U.S.C. § 2510(11) (" '[A]ggrieved person' means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.").

At the hearing, Defendant Tragas was provided an opportunity to speak with defense counsel regarding the proofs that would be necessary to establish standing. The Court advised that

---

by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection–

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

Defendant would need to establish, at a minimum, that Defendant was both the sender and the receiver of any electronic communications in order to demonstrate the necessary privacy interest. In turn, defense counsel requested fifteen to thirty days within which to conduct a forensic examination of the laptop computer. Defense counsel asserted that he sought to ascertain whether any of the electronic communications found on the computer had traveled through an Internet Service Provider ("ISP"). The Court denied the request, finding that whether the electronic communications had traveled through an ISP was not relevant when Defendant did not challenge the fact that the communications were found on the hard drive of the laptop computer and not obtained by the government from an ISP.

Based on the above, Defendant's motion to suppress will be denied.

III

Additionally, Defendant's motion to permit Defendant to access laptop computer to view discovery [Dkt. # 161], filed on February 22, 2010, will be denied. Defendant seeks to obtain a laptop computer, at her own expense, to participate in her defense and to view the voluminous discovery provided by the government on CDs or DVDs. While it may be more convenient to view the discovery on a laptop computer rather than in a printed format, Defendant has not taken any steps to ascertain whether necessary security arrangements can be made with prison officials.

Accordingly, it is **ORDERED** that Defendant's motion to suppress [Dkt. # 142] is **DENIED**.

It is further **ORDERED** that Defendant's motion to permit Defendant to access laptop computer to view discovery [Dkt. # 161] is **DENIED**.

It is further **ORDERED** that the government's supplemental brief [Dkt. # 173] is **STRICKEN** and the Clerk of the Court is **DIRECTED** to remove the images from the docket.

It is further **ORDERED** that it is **DETERMINED** that the time period from the filing of Defendant's motion to suppress [Dkt. # 142] on **January 11, 2010** to **March 16, 2010**, is **EXCLUDABLE DELAY** pursuant to 18 U.S.C.§ 3161(h)(1)(D) and (H) on the basis of actual delay.

It is further **ORDERED** that a final pretrial conference and plea cutoff is **SCHEDULED** for **April 13, 2010 at 2:30 p.m.**, and a trial is **SCHEDULED** for **April 27, 2010 at 8:30 a.m.**

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge

Dated: March 16, 2010

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney or party of record herein by electronic means or first class U.S. mail on March 16, 2010.

s/Tracy A. Jacobs
TRACY A. JACOBS